Application No.: 10/077,851   Docket No.: 1509-280

AMENDMENTS TO THE CLAIMS:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1.   (currently amended) A method of exchanging a digital credential between a first computer node and a second computer node, the method comprising

establishing a secure connection between the first node and second node over a communication network;

~~prior to conducting a transaction between the first and second nodes,~~ establishing trust or increasing the level of trust between the first and second nodes by

transferring a digital credential from the first node to the second node over the secure connection; and

after said transferring, verifying the trustworthiness of the transferred digital credential against at least one policy of the second node; [[and]]

upon a determination that the digital credential satisfies said at least one policy, conducting [[said]] a transaction between the first and second nodes over the secure connection; and

monitoring, in real time, the digital credential that has been transferred over said secure connection.

2.   (canceled)

3.   (previously presented) A method according to claim 1, wherein the digital credential is an attribute credential of an entity at the first node, said entity being a user or a system or a service.

2

Application No.: 10/077,851   **Docket No.: 1509-280**

4-5.   (canceled)

6.   (previously presented) A method according to claim 1, wherein the digital credential is an identity certificate of a user at the first node.

7-8.   (canceled)

9.   **(currently amended)** A method of exchanging a digital credential between a first computer node and a second computer node, the method comprising:

establishing a secure connection between the first node and second node over a communication network;

~~initiating, in response to the interaction of a user of a computer node on the network, the transfer of~~ transferring a digital credential from the first node to the second node over the secure connection; [[and]]

presenting to a user the digital credential associated with the secure connection <u>and enabling real time monitoring of the digital credential whilst said secure connection is active.</u>

10.   (previously presented) A computer system comprising a first computer node coupled to a second computer node via a communication network, the first node and second node being arranged to allow a secure connection to be established between the first and second nodes, the first and second nodes having processors configured to perform the method of claim 1.

11.   (previously presented) A computer system according to claim 10, wherein the processors are further configured to perform the method of claim 23.

12.   (canceled)

3

Application No.: 10/077,851   Docket No.: 1509-280

13.   (previously presented) A computer system according to claim   10, wherein the processors are further configured to perform the method of claim 20, and at least one of the first node and second node further comprises said graphical user interface.

14.   (previously presented) A computer system according to claim 11, wherein   the second node further comprises

said graphical user interface; and

a controller for allowing the user to change statuses of the digital credentials in real time.

15.   (currently amended) A computer node for coupling to a second computer node via a communication network, the computer node being arranged to allow a secure connection to be established with the second computer node, the computer node comprising a processor responsive to the interaction of a user for

receiving a digital credential from the second node over a secure connection established between the nodes;

after said receiving, verifying the trustworthiness of the received digital credential against at least one policy; [[and]]

upon a determination that the digital credential satisfies said at least one policy, conducting a transaction with said second node over the secure connection;

storing the digital credential that has been transferred over said secure connection; and

enabling real time monitoring and real time updating of a property or status of the stored digital credential whilst said secure connection is active.

16-19. (canceled)

20.   (currently amended) A method according to claim 1, further comprising

4

presenting, via a graphical user interface and in human-readable format, to a user at either or both of said first and second nodes the digital credential <u>that has been</u> transferred over the secure connection.

21.   (previously presented) A method according to claim 20, wherein said presenting comprises displaying, by said graphical user interface, properties of said digital credential on a display, said properties comprising credential type, credential issuer, credential holder, and validity period.

22.   (previously presented) A method according to claim 1, further comprising

presenting, via a graphical user interface and in human-readable format, to a user at said first node a list of credentials of said user; and

allowing the user to select at least one of the credentials from said list as the digital credential to be transferred over the secure connection.

23.   (currently amended) A method according to claim 1, further comprising

establishing a plurality of secure connections between the second node and a plurality of said first nodes over the communication network;

presenting, via a graphical user interface and in human-readable format, to a user ~~at said~~ ~~second node~~ a list of digital credentials which have been transferred over the respective secure connections and verified to be trustworthy; and

allowing the user to monitor and intervene on the credentials in real time.

24.   (previously presented) A method according to claim 23, wherein said presenting comprises displaying, by said graphical user interface, properties of at least one of said credentials of the list on a display, said properties comprising credential issuer, credential holder, and validity period.

5

25.   (currently amended) A method according to claim 1, wherein said transaction comprises providing, over the secure connection, access by the first node to a service provided by the second node;

said method further comprising:

requesting, by the first node, another digital credential from the second node;

determining, by the second node, whether the first node is entitled to the receive the requested digital credential, and, upon a positive determination, transmitting the requested digital credential from the second node to the first node over the secure connection; and

monitoring, in real time and by said second node, the requested digital credential that has been issued by said second node and transferred to said first node.

26.   (previously presented) A method according to claim 25, wherein said requesting, determining and transmitting are performed as part of said establishing trust or increasing the level of trust between the first and second nodes and are followed by

examining, by the first node, the requested digital credential received from the second node prior to the transfer of the digital credential from the first node to the second node.

27.   (previously presented) A method according to claim 25, wherein said requesting, determining and transmitting are performed after said establishing trust or increasing the level of trust between the first and second nodes and are followed by

using, by the first node, the requested digital credential received from the second node to establish trust or increase the level of trust between the first node and a third node which is coupled to said first node via the communication network and over another established secure connection.

28.   (previously presented) A computer node according to claim 15, further comprising a credential validation server module executable by the processor for executing a two-phase control

6

on the digital credential, said two-phase control comprising:

a first phase in which said credential validation server module interacts with at least one external entity to check if the digital credential is still valid; and

a second phase in which said credential validation server module verifies the trustworthiness of the received digital credential against said at least one policy by checking on at least one of explicit constraints on the validation path, the issuer of the digital credential, and the context in which the digital credential has been issued.

29. (previously presented) A computer node according to claim 28, further comprising an authorization server module executable by the processor for at least one of evaluating said at least one policy, modifying said at least one policy, and reloading the modified policy on the fly without service disruption.

30. (previously presented) A computer node according to claim 29, further comprising a credential content management module executable by the processor for

abstracting the digital credential to be a collection of attributes independent of an original format of said digital credential, and

returning the abstracted digital credential to the credential validation server module.

31. (previously presented) A computer node according to claim 30, further comprising a user context manager module executable by the processor for

receiving the abstracted digital credential from the credential validation server module, and

storing the abstracted digital credential in a user context area for an entire lifetime of said secure connection.

32. (previously presented) A computer node according to claim 31, further comprising an object pool manager module executable by the processor for dynamically managing the content

of multiple said user context areas stored by the user context manager module, wherein

said managing comprises at least one of modifying, adding, removing, and disabling one or more digital credentials stored in the user context areas, and

said authorization server module accesses one or more of the user context areas and evaluates said at least one policy against the content of said one or more of the user context areas.

33.   (new) The method of claim 1, wherein said monitoring comprises at least one of (1) checking the validity of said digital credential and (2) verifying the trustworthiness of said digital credential against said at least one policy, by said second node and either periodically or at a user's initiative.